

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 05-075597

(43)Date of publication of application : 26.03.1993

(51)Int.Cl.

H04L 9/06
H04L 9/14
G09C 1/00

(21)Application number : 03-230580

(71)Applicant : FUJITSU LTD

(22)Date of filing : 10.09.1991

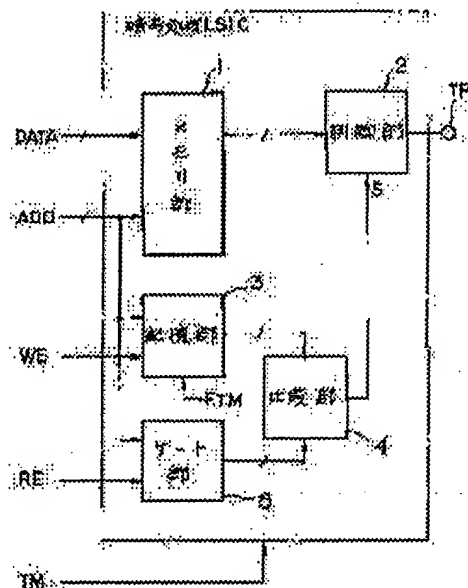
(72)Inventor : TANAKA HIDEAKI

(54) SECRET KEY PROTECTING SYSTEM AND CIPHER PROCESSING LSIC BY THIS SYSTEM

(57)Abstract:

PURPOSE: To provide the secret key protecting system and the cipher processing of this system where read/write of a memory part where secret key data is stored can be checked but secret key data cannot be observed from the external.

CONSTITUTION: Data in a memory part 1 where secret key information is stored can be read/written from the external in the test mode. A control part 2 which controls permission/inhibition of external output of read data from the memory part 1, a storage part 3 where all stored information are reset by input of a test mode signal TM and information related to addresses where data is written in the memory part 1 is stored thereafter, and a comparing part 4 which compares stored information of the storage part 3 and information related to the address for data read of the memory part 1 with each other are provided. When the test mode is set and the comparison in the comparing part 4 results in coincidence, the control part 2 permits data output. The memory part 1 and a cipher processing part which generates secret key information are unified and integrated into a cipher processing LSIC to improve the secrecy.



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision]

of rejection]

[Date of requesting appeal against examiner's
decision of rejection]

[Date of extinction of right]

Copyright (C); 1998,2003 Japan Patent Office

(19)日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11)特許出願公開番号

特開平5-75597

(43)公開日 平成5年(1993)3月26日

(51)Int.Cl. ⁵	識別記号	庁内整理番号	F I	技術表示箇所
H 0 4 L 9/06				
9/14				
G 0 9 C 1/00		9194-5L		
		7117-5K	H 0 4 L 9/ 02	Z

審査請求 未請求 請求項の数2(全 8 頁)

(21)出願番号 特願平3-230580

(22)出願日 平成3年(1991)9月10日

(71)出願人 000005223

富士通株式会社

神奈川県川崎市中原区上小田中1015番地

(72)発明者 田中 秀明

宮城県仙台市青葉区一番町1丁目2番25号

富士通東北デジタル・テクノロジー株式
会社内

(74)代理人 弁理士 井桁 貞一

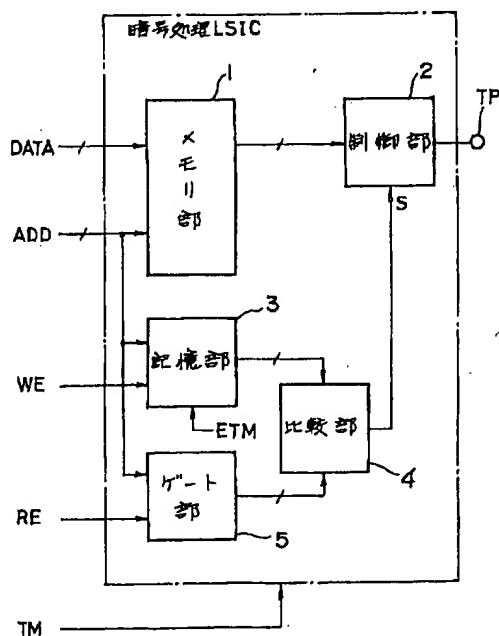
(54)【発明の名称】 秘密鍵保護方式及び該方式による暗号処理LSIC

(57)【要約】

【目的】 本発明は秘密鍵保護方式及び該方式による暗号処理LSICに関し、秘密鍵データを記憶するメモリ部の読み/書き検査が可能であると共に外部からは秘密鍵データを観測できない秘密鍵保護方式及び該方式による暗号処理LSICの提供を目的とする。

【構成】 テストモードにより秘密鍵情報を記憶するメモリ部1のデータを外部から読み/書き可能に構成された装置の秘密鍵保護方式において、メモリ部1の読出データの外部出力可否を制御する制御部2と、テストモード信号TMの投入により全記憶情報がリセットされて、その後のメモリ部1へのデータ書込を行ったアドレスに係る情報を記憶する記憶部3と、記憶部3の記憶情報とメモリ部1のデータ読出を行うアドレスに係る情報とを比較する比較部4とを備え、テストモードでかつ比較部4の比較一致が得られたことにより制御部2を出力可にする。またメモリ部1と秘密鍵情報を発生する暗号処理部とを一体化、集積化して暗号処理LSICとなし、秘密性を向上させる。

本発明の原理的構成図



【特許請求の範囲】

【請求項1】 テストモードにより、秘密鍵に係る情報を記憶するメモリ部(1)のデータを外部から読み書き可能に構成された装置の秘密鍵保護方式において、メモリ部(1)の読出データの外部への出力可否を制御する制御部(2)と、

テストモード信号(TM)の投入により全記憶情報がリセットされて、その後のメモリ部(1)へのデータの書き込みを行ったアドレスに係る情報を記憶する記憶部(3)と、

記憶部(3)の記憶情報とメモリ部(1)のデータの読み出しを行うアドレスに係る情報とを比較する比較部(4)とを備え、

テストモードでかつ比較部(4)の比較一致が得られたことにより制御部(2)を出力可にすることを特徴とする秘密鍵保護方式。

【請求項2】 テストモードにより、秘密鍵に係る情報を記憶するメモリ部(1)のデータを外部から読み書き可能に構成された記憶装置を備える暗号処理LSICにおいて、

メモリ部(1)の読出データの外部端子(TP)への出力可否を制御する制御部(2)と、

テストモード信号(TM)の投入により全記憶情報がリセットされて、その後のメモリ部(1)へのデータの書き込みを行ったアドレスに係る情報を記憶する記憶部(3)と、

記憶部(3)の記憶情報とメモリ部(1)のデータの読み出しを行うアドレスに係る情報とを比較する比較部(4)とを備え、

テストモードでかつ比較部(4)の比較一致が得られたことにより制御部(2)を出力可にするように構成されたことを特徴とする暗号処理LSIC。

【発明の詳細な説明】

【0001】

【産業上の利用分野】 本発明は秘密鍵保護方式及び該方式による暗号処理LSICに関し、更に詳しくは、テストモードにより、秘密鍵に係る情報を記憶するメモリ部のデータを外部から読み書き可能に構成され装置の秘密鍵保護方式及び該方式による暗号処理LSICに関する。

【0002】 近年、社会の高度情報化に伴い、データのセキュリティ保護が強く望まれており、暗号処理の重要性が高まっている。従って、かかる暗号処理の中核を担う秘密鍵情報を記憶する装置又はこれに暗号処理部を一体化して集積化した暗号処理LSICにおいては、鍵データの秘密管理が極めて重要であり、仮に、このLSIC等を搭載した装置が盗まれて、動作が解析されようとしても、秘密の鍵データが外部に取り出せないことが重要である。

【0003】

【従来の技術】 図4は従来の暗号処理LSICのブロック図で、図において、10は移動通信端末に組み込まれた暗号処理LSIC、11はNTTのFEAL-8暗号アルゴリズムに従う鍵処理部、12はセクタ部、13はメモリ部、14は同FEAL-8暗号アルゴリズムに従うデータランダム化部、15はトライステートのバッファ回路である。

【0004】 通常の動作モードでは、テストモード信号TMはLOWレベルであり、これによってセクタ部12は入力端子のA側を選択し、かつバッファ回路15の出力TPはハイインピーダンスである。この状態で、予め、基地局からは64ビット長の鍵データKDが秘密に送られる。鍵処理部11は、この鍵データKDをFEAL-8暗号アルゴリズムに従って混ぜ合わせることで暗号強度を増した256ビット長の拡大鍵データEKDを生成し、これをメモリ部13に格納する。

【0005】 次に、基地局又は移動通信端末内の不図示のCPUから64ビット長の平文データMDが送られる。データランダム化部14は、この平文データMDとメモリ部13の拡大鍵データEKDとをFEAL-8暗号アルゴリズムに従って混ぜ合わせることでさらに暗号強度を増した暗号データCDを生成し、これを外部に出力する。そして、図示しないが、外部においてサンプリング量子化された音声データは、データランダム化部14の暗号データCDによって暗号化され、無線送信される。

【0006】 ところで、このようなFEAL-8暗号アルゴリズムは一般に公開されるものである。しかも、同一の暗号処理LSICが多く市場に出回るので、誰でも入手可能になる。従って、このようなLSICを搭載した装置が盗まれた場合には、暗号化動作が解析されてしまうという恐れが生じる。しかし、仮に平文データMDが知られてしまっても、拡大鍵データEKDが知られない限りは音声データを復号化できない。しかも、お元の鍵データKDは秘密に送られるものであり、この鍵データKDを知らない限りは拡大鍵データEKDを生成できない。従って、このような暗号処理LSICを使用した暗号処理システムは一見安全である。

【0007】 しかるに、一般に、この種の暗号処理LSICではメモリ部13の記憶動作が正常に行われるか否かを調べる必要があり、このためにメモリ部13のデータ読み書きをテストするテストモードが設けられている。このテストモードでは、テストモード信号TMはHIGHレベルであり、これによってセクタ部12は入力端子のB側を選択し、かつバッファ回路15の出力はその入力に応じて変化する。即ち、テストモードでは、外部から任意のアドレスTAにテストデータTDを書き込み、あるいは任意のアドレスTAのデータをテスト端子TPに読み出すことが可能である。従って、従来の暗号処理LSICでは、テストモード信号TMをHIGH

レベルにすることで秘密の拡大鍵データEKDを容易に
知ることができた。

【0008】

【発明が解決しようとする課題】上記のように従来の暗
号処理LSICでは、該LSICをテストモードにする
ことにより外部から容易に秘密の拡大鍵データを観測で
きるので、通信を盗聴される恐れがあった。本発明の目
的は、外部から秘密鍵データを記憶するメモリ部の読み
／書き検査が可能であると共に、外部からは秘密鍵デー
タが観測できない秘密鍵保護方式及び該方式による暗号
処理LSICを提供することにある。

【0009】

【課題を解決するための手段】上記の課題は図1の構成
により解決される。即ち、本発明の秘密鍵保護方式は、
テストモードにより、秘密鍵に係る情報を記憶するメモ
リ部1のデータを外部から読み／書き可能に構成された
装置の秘密鍵保護方式において、メモリ部1の読出デー
タの外部への出力可否を制御する制御部2と、テストモ
ード信号TMの投入により全記憶情報がリセットされ
て、その後のメモリ部1へのデータの書き込みを行った
アドレスに係る情報を記憶する記憶部3と、記憶部3の
記憶情報とメモリ部1のデータの読み出しを行うアドレ
スに係る情報とを比較する比較部4とを備え、テストモ
ードでかつ比較部4の比較一致が得られたことにより制
御部2を出力可にするものである。

【0010】また、本発明の暗号処理LSICは、テスト
モードにより、秘密鍵に係る情報を記憶するメモリ部
1のデータを外部から読み／書き可能に構成された記憶
装置を備える暗号処理LSICにおいて、メモリ部1の
読出データの外部端子TPへの出力可否を制御する制御
部2と、テストモード信号TMの投入により全記憶情報
がリセットされて、その後のメモリ部1へのデータの書
き込みを行ったアドレスに係る情報を記憶する記憶部3
と、記憶部3の記憶情報とメモリ部1のデータの読み出
しを行うアドレスに係る情報とを比較する比較部4とを
備え、テストモードでかつ比較部4の比較一致が得られ
たことにより制御部2を出力可にするように構成されて
いる。

【0011】

【作用】本発明の秘密鍵保護方式においては、テストモ
ード信号TMの投入によりそのエッジ信号ETMで記憶
部3の全記憶内容がリセットされる。そして、その後に
メモリ部1に対して何らかのテストデータDATAの書
き込みを行うと、その際の書込イネーブル信号WEによ
ってその際の書込アドレスADDに係る情報が記憶部3
に記憶される。こうして、メモリ部1の任意アドレスA
DDに任意データDATAを書き込むことが可能であ
り、各書込毎にその書込アドレスADDに係る情報が記
憶部3に記憶される。

【0012】また、このテストモードでメモリ部1に対

してデータDATAの読み出しを行うと、ゲート部5は
その際の読出イネーブル信号REによってその際の読出
アドレスADDに係る情報を出力する。そして、比較部
4は記憶部3の書込アドレスに係る情報とゲート部5の
読出アドレスに係る情報とを比較しており、比較の一致
が得られると制御部2を出力可にし、それ以外は出力不
可にする。

【0013】従って、テストモードへの投入後は、メモ
リ部1に何らかのデータを書き込んだ場合はそのアドレ
スのデータを外部TPに読み出せるが、データを書き込
まなかったアドレスのデータ、即ち、秘密鍵に係るデー
タは外部TPには読み出せない。かくして、本発明によ
れば、暗号処理LSICをテストモードにすることによ
りメモリ部1の読み／書き検査を行うことは可能である
が、秘密の鍵データを外部に読み出すことはできない。

【0014】また本発明の暗号処理LSICにおいて
は、テストモードにより、秘密鍵に係る情報を記憶する
メモリ部1のデータを外部から読み／書き可能に構成さ
れた記憶装置と、この秘密鍵に係る情報を生成等する暗
号処理部とを一体化、集積化することで暗号処理装置の
秘匿性を一層高めている。

【0015】

【実施例】以下、添付図面に従って本発明による実施例
を詳細に説明する。図2は実施例の暗号処理LSICの
ブロック図で、図において20は移動通信端末に組み込
まれた実施例の暗号処理LSIC、11はNTTのFEA
L-8暗号アルゴリズムに従う鍵処理部、12はセレ
クタ部、13はメモリ部（図1の1に相当）、14は同
FEAL-8暗号アルゴリズムに従うデータランダム化
部、15はトライステートのバッファ回路（同2に相
当）、8は秘密鍵保護部（同3～5に相当）である。

【0016】通常の動作モードでは、テストモード信号
TMはLOWレベルであり、これによってセレクタ部1
2は入力端子のA側を選択し、かつバッファ回路15の
出力TPはハイインピーダンスである。この状態で、予
め、基地局からは64ビット長の鍵データKDが秘密に
送られる。鍵処理部11は、この鍵データKDをFEA
L-8暗号アルゴリズムに従って混ぜ合わせることで暗
号強度を増した256ビット長の拡大鍵データEKDを
生成し、これをメモリ部13に格納する。

【0017】次に、基地局又は移動通信端末内の不図示
のCPUから64ビット長の平文データMDが送られ
る。データランダム化部14は、この平文データMDと
メモリ部13の拡大鍵データEKDとをFEAL-8暗
号アルゴリズムに従って混ぜ合わせることでさらに暗号
強度を増した暗号データCDを生成し、これを外部に出
力する。そして、図示しないが、外部においてサンプリ
ング量子化された音声データは、データランダム化部1
4の暗号データCDによって暗号化され、無線送信され
る。

【0018】またテストモードでは、テストモード信号TMはHIGHレベルであり、これによりセクタ部12は入力端子のB側を選択し、かつバッファ回路15は後述の秘密鍵保護部8の制御信号Sによって制御されることになる。図3は実施例の秘密鍵保護部のブロック図で、図において81、82はデコーダ、83はラッチ回路、84はAND-ORゲート回路から成る比較部、85は遅延インバータ素子、86、87はANDゲート回路である。なお、デコーダ81及びラッチ回路83は図1の記憶部3に相当し、デコーダ82は同ゲート部5に相当し、比較部84は同比較部4に相当する。

【0019】テストモード信号TMが投入されると、その立ち上がり部分を遅延インバータ素子85及びANDゲート回路86で抽出したエッジ信号ETMが発生し、これによりラッチ回路83の全出力 $Q_0 \sim Q_n$ がリセットされる。そして、その後にメモリ部1に対して何らかのテストデータの書き込みが行われると、その際の書込イネーブル信号WEによってその際の書込アドレスADDをデコードした信号 $A_0 \sim A_n$ の何れか一つが発生し、これがラッチ回路83の対応するビットをセットする。こうして、メモリ部1の任意アドレスADDに任意データDATAを書き込むことが可能であり、各書込毎にその書込アドレスADDをデコードした信号 $A_0 \sim A_n$ の何れか一つが発生し、これがラッチ回路83の対応するビットをセットする。

【0020】また、メモリ部1に対してデータの読み出しを行うと、デコーダ82はその際の読出イネーブル信号REによってその際の読出アドレスADDをデコードした信号 $A_0 \sim A_n$ の何れか一つを発生する。この状態で、比較部84はラッチ回路83の出力信号 $Q_0 \sim Q_n$ とデコーダ82の出力信号 $A_0 \sim A_n$ との各AND-OR論理をとっている。

【0021】例えば、今、デコーダ82の出力信号 A_0 がHIGHレベルの時に、ラッチ回路83の出力信号 Q_0 がHIGHレベルの時は、このアドレスについては既にテストデータの書き込みが行われており、比較部84はHIGHレベルを出力する。また、デコーダ82の出力信号 A_n がHIGHレベルの時に、ラッチ回路83の出力信号 Q_n がLOWレベルの時は、このアドレスについては未だテストデータの書き込みが行われておらず、

比較部84はLOWレベルを出力する。

【0022】そして、ANDゲート回路87にはテストモード信号TMが入力しているため、結局、秘密鍵保護部8はテストモードでかつ比較部84の比較一致が得られた時のみHIGHレベルの制御信号Sを出力し、バッファ回路15は制御信号SがHIGHレベルの時のみメモリ部1の読出データを外部端子TPに出力する。なお、上記実施例では暗号処理LSICを移動通信端末に組み込んだ場合を示したが、他のいかなる暗号処理装置にも適用可能である。

【0023】また、上記実施例ではNTTのFEAL-8暗号アルゴリズムに従う暗号処理を示したが、他の暗号アルゴリズムに従う暗号処理にも適用可能である。

【0024】

【発明の効果】以上述べた如く本発明によれば、メモリ部1の読出データの外部への出力可否を制御する制御部2と、テストモード信号TMの投入により全記憶情報がリセットされて、その後のメモリ部1へのデータの書き込みを行ったアドレスに係る情報を記憶する記憶部3と、記憶部3の記憶情報とメモリ部1のデータの読み出しを行うアドレスに係る情報とを比較する比較部4とを備え、テストモードでかつ比較部4の比較一致が得られたことにより制御部2を出力可にするので、外部からメモリ部1の読み書き検査が可能であると共に、外部からは秘密鍵の盗難による悪用を防止することができる。

【図面の簡単な説明】

【図1】図1は本発明の原理的構成図である。

【図2】図2は実施例の暗号処理LSICのブロック図である。

【図3】図3は実施例の秘密鍵保護部のブロック図である。

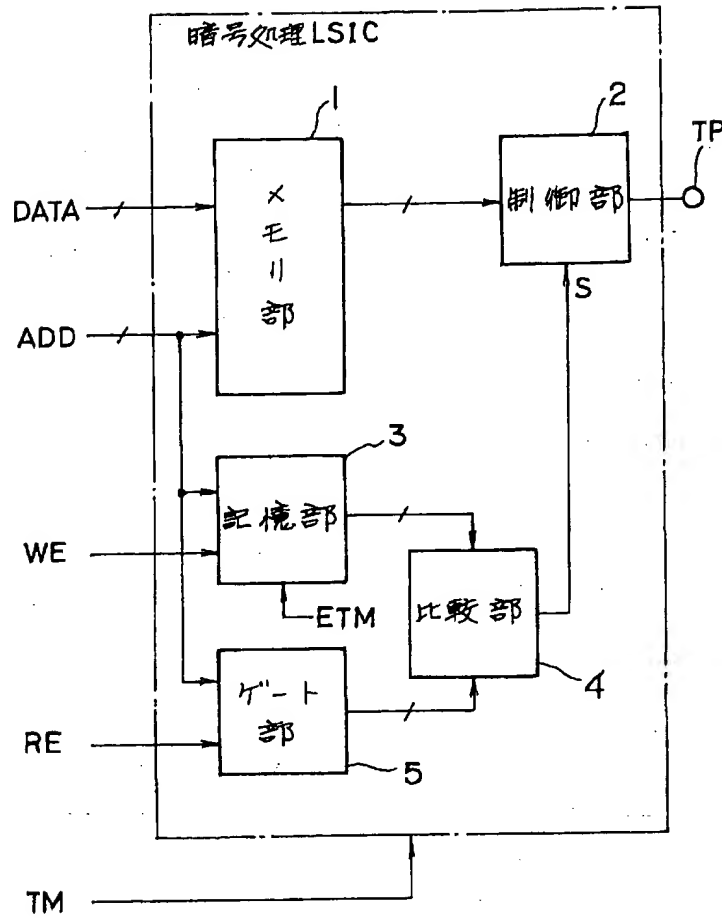
【図4】図4は従来の暗号処理LSICのブロック図である。

【符号の説明】

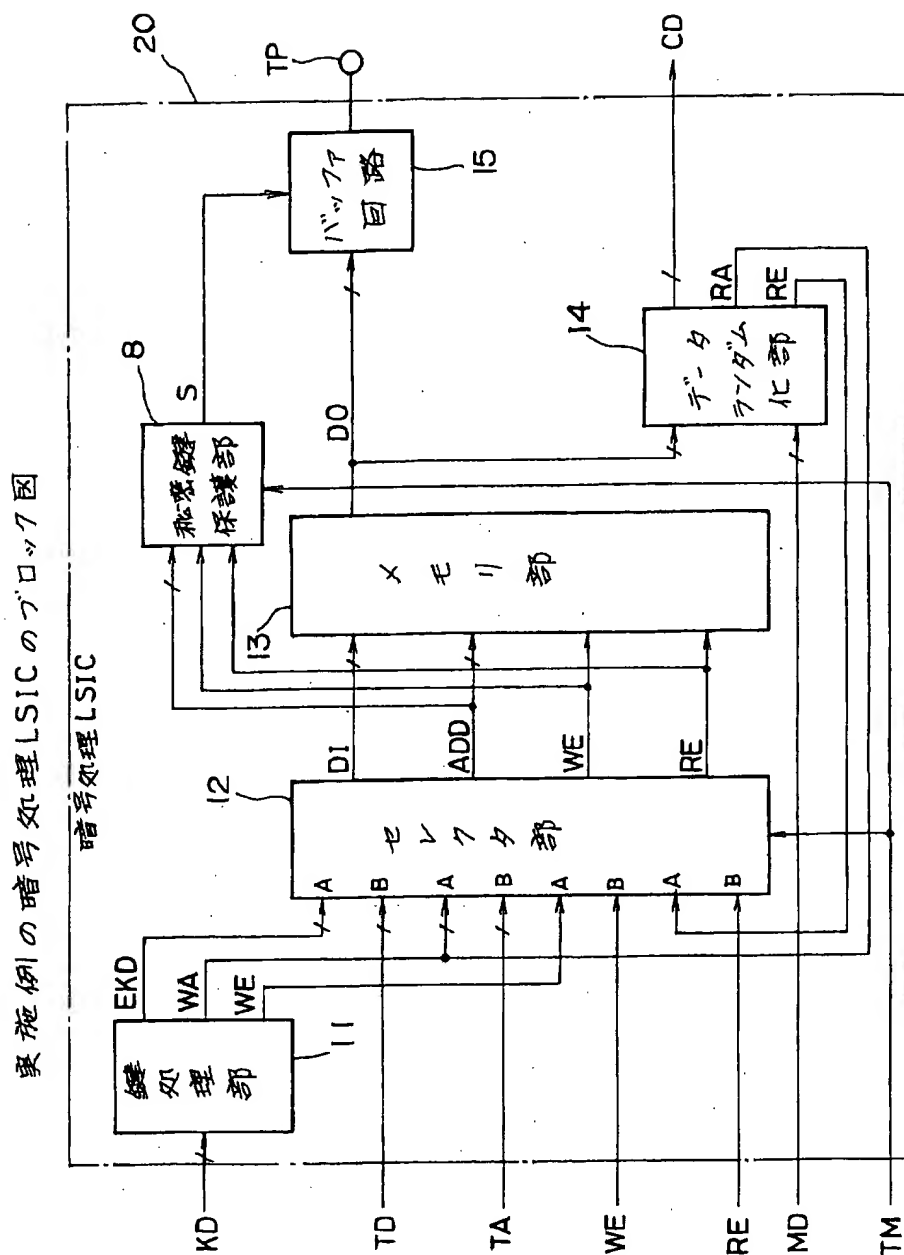
- 1 メモリ部
- 2 制御部
- 3 記憶部
- 4 比較部
- 5 ゲート部

【図1】

本発明の原理的構成図

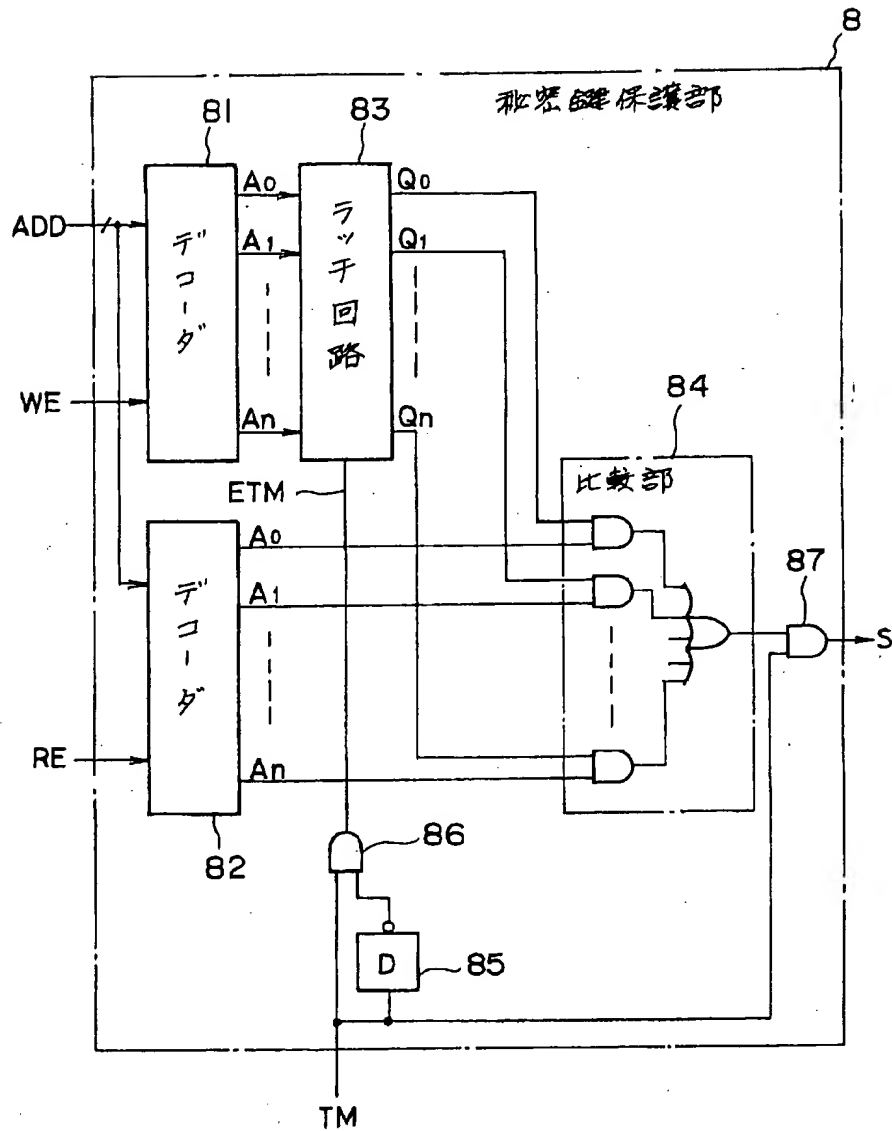


【図2】



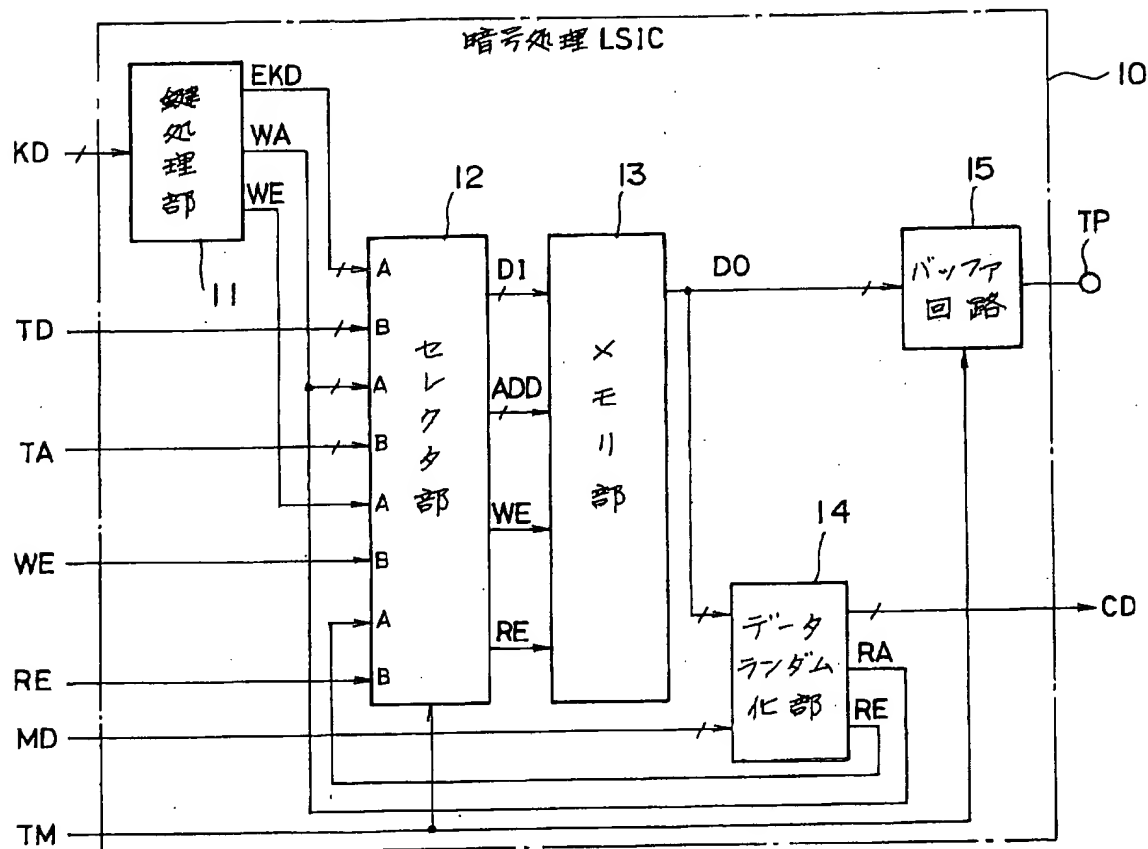
【図3】

実施例の秘密鍵保護部のブロック図



【図4】

従来の暗号処理LSICのブロック図



**This Page is Inserted by IFW Indexing and Scanning
Operations and is not part of the Official Record**

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- ☐ BLACK BORDERS
- ☐ IMAGE CUT OFF AT TOP, BOTTOM OR SIDES
- ☐ FADED TEXT OR DRAWING
- ☐ BLURRED OR ILLEGIBLE TEXT OR DRAWING
- ☐ SKEWED/SLANTED IMAGES
- ☒ COLOR OR BLACK AND WHITE PHOTOGRAPHS
- ☐ GRAY SCALE DOCUMENTS
- ☒ LINES OR MARKS ON ORIGINAL DOCUMENT
- ☐ REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY
- ☐ OTHER: _____

IMAGES ARE BEST AVAILABLE COPY.

As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.